



SERVIDOR PROXY

Robert Lita Jeler, Irene Arias Rodríguez, Astrid Katiuska Arenales Cádiz – Formación
Profesional Grado Superior
2º Administración en Sistemas Informáticos y Redes
Servicios de Red e Internet

ÍNDICE

INTRODUCCIÓN.....	3
ASPECTOS CLAVE DE LA MEMORIA	3
¿QUÉ ES UN SERVIDOR PROXY Y A QUÉ SE DEDICA?	5
VENTAJAS DE UN SERVIDOR PROXY (TESTDEVELOCIDAD, S.F.)	5
DESVENTAJAS DE UN SERVIDOR PROXY	5
GUÍA DE INSTALACIÓN DE SERVIDOR PROXY	5
CONFIGURACIÓN DE MÁQUINAS VIRTUALES	5
INSTALACIÓN DE SQUID.....	8
BLOQUEO DE PÁGINAS	10
IMPLEMENTACIÓN DE PROXY EN NAVEGADOR	10
MODIFICACIÓN DE PÁGINA ERROR	12
INSTALACIÓN Y CONFIGURACIÓN DE SQUIDGUARD	14
CONCLUSIÓN.....	17
BIBLIOGRAFÍA	18

INTRODUCCIÓN

En el presente trabajo se ha llevado a cabo la implementación y configuración de un servidor proxy utilizando **Squid** en un entorno Linux, con el objetivo de gestionar y optimizar el acceso a Internet desde una red interna. A lo largo del proyecto se han abordado diferentes aspectos de la configuración de Squid, como la definición de reglas de control de acceso, la restricción de dominios específicos, y la correcta integración con los navegadores de los clientes de la red, como Firefox. Además, se ha añadido una capa adicional de seguridad y filtrado mediante la inclusión de **SquidGuard**, un plugin ampliamente utilizado para la creación de listas negras de sitios web y el filtrado de contenido.

ASPECTOS CLAVE DE LA MEMORIA

- **Configuración inicial de Squid:** el proyecto se inició con la instalación y configuración básica de Squid como proxy HTTP y HTTPS. Esta fase incluyó la definición de ACLs (Listas de Control de Acceso) para permitir el acceso desde redes internas específicas, así como la configuración de puertos y dominios permitidos y bloqueados.
- **Gestión de acceso a sitios web:** a continuación, se procedió a crear reglas de control de acceso para restringir el uso de determinados dominios y protocolos, asegurando que solo se pudiera acceder a ciertos servicios web autorizados. Esto se logró mediante la creación de ACLs que especifican dominios permitidos y la posterior integración de listas negras para bloquear sitios no deseados, como YouTube y Facebook.
- **Implementación de SquidGuard:** para ampliar la funcionalidad de filtrado de Squid, se integró SquidGuard, que permite aplicar políticas de control de acceso basadas en categorías de sitios web y listas negras. Se configuraron listas negras para bloquear categorías completas de sitios (por ejemplo, contenido para adultos, redes sociales y sitios de juegos), asegurando una navegación segura y controlada.
- **Pruebas de conectividad y resolución de problemas:** Durante el desarrollo, se presentaron problemas de conectividad debido a configuraciones incorrectas tanto en las ACLs como en la configuración de los navegadores. Estos inconvenientes fueron resueltos mediante el ajuste de las reglas de acceso, asegurando que el servidor proxy gestionara correctamente las solicitudes de los clientes y rechazara las conexiones no autorizadas.
- **Configuración de DNS y rutas de red:** para un correcto enrutamiento y resolución de nombres de dominio, se configuró el servidor proxy para utilizar un DNS externo (como Google DNS, 8.8.8.8). Esto garantizó que las solicitudes de los clientes se procesaran de manera eficiente y que las páginas bloqueadas fueran correctamente identificadas por el proxy.
- **Seguridad y control de tráfico:** se implementaron políticas de seguridad adicionales para evitar accesos no deseados al servidor proxy, como la restricción de acceso a puertos específicos y la denegación de acceso desde direcciones IP no autorizadas. Estas medidas refuerzan la seguridad de la red, protegiendo tanto a los clientes como al propio servidor de accesos no controlados.

- **Documentación de la configuración:** finalmente, se ha documentado cada paso del proceso de implementación, detallando la configuración utilizada, las pruebas realizadas y las soluciones aplicadas a los problemas encontrados.

¿QUÉ ES UN SERVIDOR PROXY Y A QUÉ SE DEDICA?

Un servidor **proxy** (Wikipedia, s.f.) es un equipo que actúa como intermediario entre un cliente (como un navegador web) y un servidor. Recibe las solicitudes del cliente, las reenvía al servidor y devuelve las respuestas, almacenadas en caché para reducir tiempos de carga y mejorar el rendimiento de la red.

Además de mejorar la velocidad, los proxies ofrecen **seguridad** y **control** sobre el acceso a recursos, permitiendo bloquear contenido o aplicar políticas de acceso. Ocultan la dirección IP del cliente para garantizar **anonimato** y **protección de la privacidad**. También filtran contenido, detectan amenazas y optimizan el tráfico con técnicas como la compresión.

Existen diferentes tipos de proxy, como el **proxy web** (el más común), que mejora la seguridad y el anonimato durante la navegación. Pueden estar instalados localmente o en servidores externos.

VENTAJAS DE UN SERVIDOR PROXY (*testdevelocidad, s.f.*)

- **Anonimato y privacidad:** disfraza la dirección IP del equipo cliente al hacer peticiones en la web, lo que protege a los usuarios de amenazas externas
- **Mejora el rendimiento:** almacena en caché el contenido web, reduciendo así la carga en el equipo que realiza las peticiones.
- **El equipo no está restringido geográficamente:** el proxy puede anunciar el lugar de conexión del cliente como si este último se encontrase en otro país, por lo que se puede acceder a contenido que pueda estar restringido en otras áreas.

DESVENTAJAS DE UN SERVIDOR PROXY

- **Requiere configuración y mantenimiento:** Dejando de lado el proceso de configuración inicial, que puede resultar desafiante o tedioso, el proxy se debe revisar casi a diario para comprobar que funcione correctamente.
- **Problemas de compatibilidad:** Algunas páginas web pueden presentar problemas de uso si la petición se realiza por medio de un proxy.
- **Interceptación del tráfico:** Al recibir el proxy todas las peticiones de los equipos de la red, si un atacante consiguiera hacerse con él, podría interceptar el tráfico de la red de manera más fácil.

GUÍA DE INSTALACIÓN DE SERVIDOR PROXY

CONFIGURACIÓN DE MÁQUINAS VIRTUALES

Lo primero de todo vamos a configurar las máquinas virtuales. Necesitamos por lo menos dos: un servidor y un cliente. El servidor va a ser Ubuntu Linux en la versión 24.04 Desktop LTE y el cliente va a ser el mismo Linux con la misma versión.



Una vez tengamos las máquinas instaladas y configuradas con una configuración inicial, vamos a conectarlas a través de una red interna. El rango de direcciones IP va a ser **172.16.10.X**

En el servidor realizaremos dos configuraciones: **para el primer adaptador, adaptador puente; para el segundo, red interna.**

```
pc@pc-1:~$ sudo nano /etc/netplan/00-installer-config.yaml
```

```

GNU nano 7.2 /etc/netplan/00-installer-config.yaml *
network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 172.16.10.1/24
      gateway4: 172.16.10.1
      nameservers:
        addresses:
          - 8.8.8.8
    enp0s8:
      dhcp4: yes
      optional: true
  
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer
 ^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea M-E Rehacer

Si aplicamos la configuración y nos aparece el siguiente mensaje:

```
** (process:3646): WARNING **: 20:28:40.077: Permissions for /etc/netplan/01-net
work-manager-all.yaml are too open. Netplan configuration should NOT be accessib
le by others.
```

Realizaremos la siguiente configuración:

```
pc@pc-1:~$ ls -l /etc/netplan/
total 12
-rw-r--r-- 1 root root 249 sep 17 20:27 00-installer-config.yaml
-rw-r--r-- 1 root root 104 ago 27 17:42 01-network-manager-all.yaml
-rw----- 1 root root 391 sep 17 13:14 50-cloud-init.yaml
pc@pc-1:~$ sudo chmod 600 /etc/netplan/00-installer-config.yaml
pc@pc-1:~$ sudo chmod 600 /etc/netplan/01-network-manager-all.yaml
pc@pc-1:~$ ls -l /etc/netplan/
total 12
-rw----- 1 root root 249 sep 17 20:27 00-installer-config.yaml
-rw----- 1 root root 104 ago 27 17:42 01-network-manager-all.yaml
-rw----- 1 root root 391 sep 17 13:14 50-cloud-init.yaml
pc@pc-1:~$ sudo netplan apply
pc@pc-1:~$
```

Lo que estamos haciendo es quitar los permisos de lectura a los demás usuarios, siendo únicamente accesible por el usuario 'root'.

Verificamos que la conectividad funcione, haciendo ping a la dirección 172.16.10.1

```
pc@pc-1:~$ sudo netplan apply
pc@pc-1:~$ ping 172.16.10.1
PING 172.16.10.1 (172.16.10.1) 56(84) bytes of data.
64 bytes from 172.16.10.1: icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from 172.16.10.1: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 172.16.10.1: icmp_seq=3 ttl=64 time=0.020 ms
^C
--- 172.16.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 0.020/0.044/0.091/0.032 ms
pc@pc-1:~$
```

Podemos concluir que la conectividad a la red de la primera máquina virtual se ha resuelto.

Configuraremos la red en la segunda máquina virtual de Ubuntu Linux 24.04 Desktop LTE:


```

pc@pc-1: ~
GNU nano 7.2 /etc/netplan/00-installer-config.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 172.16.10.2/24
      routes:
        - to: 0.0.0.0/0
          via: 172.16.10.1
      nameservers:
        addresses:
          - 8.8.8.8

[ 14 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea
  
```

Seguimos los pasos anteriores para aplicar el plan de internet. Confirmamos que podemos hacer ping desde el cliente al servidor.

```

pc@pc-1:~$ ping 172.16.10.1
PING 172.16.10.1 (172.16.10.1) 56(84) bytes of data.
64 bytes from 172.16.10.1: icmp_seq=1 ttl=64 time=1.77 ms
64 bytes from 172.16.10.1: icmp_seq=2 ttl=64 time=0.550 ms
64 bytes from 172.16.10.1: icmp_seq=3 ttl=64 time=0.511 ms
64 bytes from 172.16.10.1: icmp_seq=4 ttl=64 time=0.438 ms
^C
--- 172.16.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3163ms
rtt min/avg/max/mdev = 0.438/0.816/1.767/0.550 ms
pc@pc-1:~$
  
```

INSTALACIÓN DE SQUID

Una vez realizada la conectividad de las máquinas virtuales, vamos a proceder con la instalación (*Clouding.io, s.f.*) y la configuración del servidor squid proxy. Esta vez vamos a utilizar un **nuevo** rango de direcciones IPv4, que va a ser la **172.16.111.X**

1. Instalaremos el servicio:
 - a. `sudo apt update`
 - b. `sudo apt install squid -y`


```
Configurando squid-langpack (20220130-1) ...
Configurando libdbi-perl:amd64 (1.643-4build3) ...
Configurando libcap3:amd64 (1.0.1-3.4ubuntu2) ...
Configurando squid-common (6.6-1ubuntu5.1) ...
Configurando squid (6.6-1ubuntu5.1) ...
Setcap worked! /usr/lib/squid/pinger is not suid!
Skipping profile in /etc/apparmor.d/disable: usr.sbin.squid
Created symlink /etc/systemd/system/multi-user.target.wants/squid.service → /usr/lib/systemd/system/squid.service.
Procesando disparadores para ufw (0.36.2-6) ...
Procesando disparadores para man-db (2.12.0-4build2) ...

Progreso: [ 95%] [#####...]
```

2. Una vez instalado, vamos a configurar el squid para que funcione como proxy para nuestra red interna:

- a. `sudo nano /etc/squid/squid.conf`
- b. Buscaremos la sección que comienza con `http_access deny all` y descomentamos esa línea quitando el `#` del inicio.

```
GNU nano 7.2 /etc/squid/squid.conf
# following rule (and/or add rules that match your definition of "local"):
# http_access allow localnet

# And finally deny all other access to this proxy
http_access deny all

# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
#
#     Essentially identical to http_access, but runs after redirectors
```

- c. Permitiremos el acceso desde nuestra red interna (**172.16.111.0/24**). Agregaremos la siguiente línea después de las directivas de `acl`:

```
acl localnet src 172.16.111.0/24
```

```
http_access allow localnet
http_access allow SSL_ports
```

- d. Confirmamos que el puerto de `http` en el que el squid escucha es al 3128 (por defecto, ya estará puesto en dicho puerto).

```
#  
  
# Squid normally listens to port 3128  
http port 3128  
  
# TAG: https_port
```

3. Guardamos el archivo y reiniciamos el servicio:

- a. `sudo systemctl restart squid`
- b. Comprobaremos que el squid esté funcionando correctamente.

```
pc@pc-1:~$ sudo systemctl restart squid.service  
pc@pc-1:~$ squid -k parse  
2024/09/17 21:01:32| Processing Configuration File: /etc/squid/squid.conf (depth 0)  
2024/09/17 21:01:32| Processing: acl SSL_ports port 443  
2024/09/17 21:01:32| Processing: acl Safe_ports port 80 # http  
2024/09/17 21:01:32| Processing: acl Safe_ports port 21 # ftp  
2024/09/17 21:01:32| Processing: acl Safe_ports port 443 # https  
2024/09/17 21:01:32| Processing: acl Safe_ports port 70 # gopher  
2024/09/17 21:01:32| Processing: acl Safe_ports port 210 # wais  
2024/09/17 21:01:32| Processing: acl Safe_ports port 1025-65535 # unregistered ports  
2024/09/17 21:01:32| Processing: acl Safe_ports port 280 # http-mgmt
```

BLOQUEO DE PÁGINAS

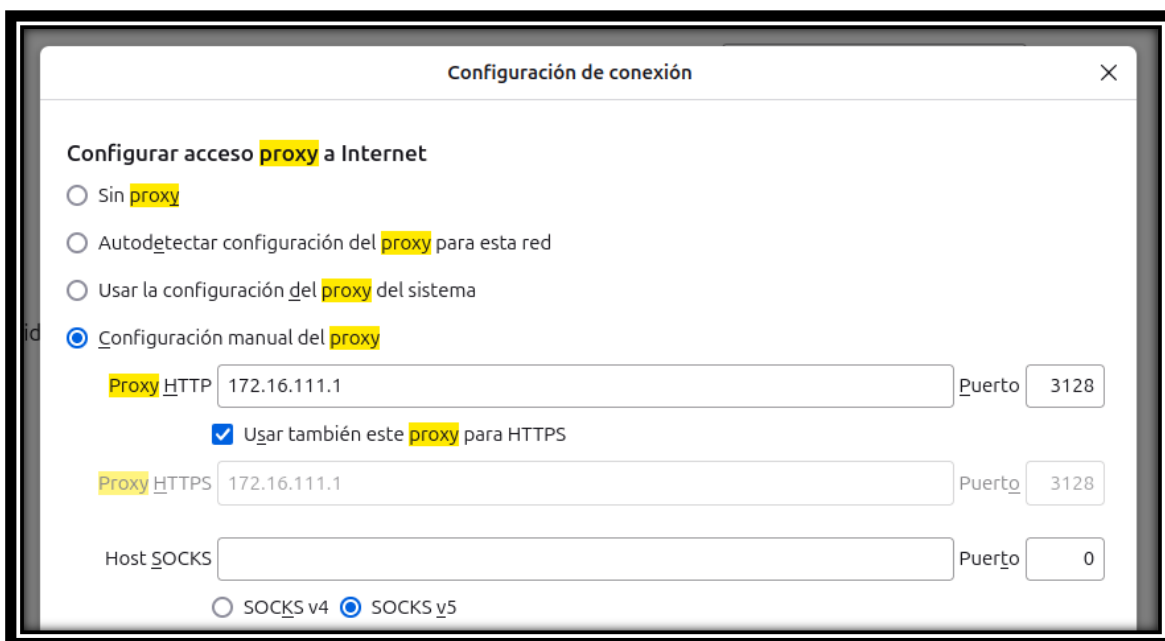
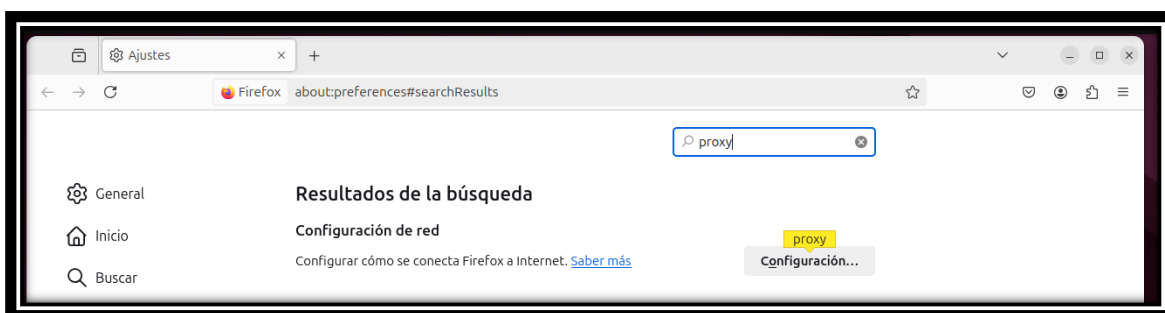
Para bloquear páginas (*ProfeSantiago, s.f.*), en la configuración insertaremos los acl correspondientes. Vamos a bloquear tres páginas: YouTube, Facebook y el aula virtual del colegio.

```
acl backlist1 dstdomain youtube.com  
acl backlist2 dstdomain facebook.com  
acl backlist3 dstdomain aula.salesianosatocha.es  
http_access deny backlist1  
http_access deny backlist2  
http_access deny backlist3
```

Utilizamos la sentencia **acl <nombre> dstdomain <dominio>** para nombrar los enlaces por acl. Una vez hayamos nombrado los enlaces (en este caso, **backlist1, 2, 3...**) vamos a denegar el acceso http utilizando la sentencia **http_access deny <nombre>**.

IMPLEMENTACIÓN DE PROXY EN NAVEGADOR

Para este apartado vamos a utilizar el navegador por defecto que viene instalado en nuestro sistema operativo Linux. En la configuración del navegador buscamos proxy, implantamos la configuración y comprobamos que funcione.



Una vez aplicada la configuración, vamos a comprobar que el proxy esté funcionando correctamente.



Como podemos observar, nos está denegando el acceso a la página del aula virtual del colegio, siéndonos imposible que podamos acceder a ella y que podamos subir prácticas o realicemos los exámenes correspondientes. Todo ello gracias a la configuración del servidor squid proxy.

MODIFICACIÓN DE PÁGINA ERROR (MEJORA)

Otro de los aspectos de esta memoria es que también podemos modificar la página de error (*Ugustavo, s.f.*) que nos aparecerá cada vez que intentemos acceder a un enlace. Veamos un ejemplo con el siguiente código HTML5:

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-
scale=1.0">
  <title>Error de Acceso Denegado</title>
  <style>
  body {
    background-image: url('');
    background-size: cover;
    background-attachment: fixed;
    font-family: 'Arial', sans-serif;
    color: #FFF;
    text-align: center;
    margin: 0;
  }
  .error-container {
    background-color: red;
    border-radius: 20px;
    padding: 30px;
    box-shadow: 0 0 20px black;
    margin: 100px auto;
    max-width: 500px;
  }
  h1 {
    color: #FFF;
    font-size: 36px;
    margin-bottom: 10px;
  }
  p {
    font-size: 18px;
    margin-bottom: 20px;
  }
  a {
    color: #3498DB;
    text-decoration: none;
    font-weight: bold;
  }
  a:hover {
    text-decoration: underline;
  }
}
```

```
.proxy-image {
    width: 150px;
    height: 150px;
}

</style>
</head>
<body>
    <div class="error-container">
        
        <h1>Error de Acceso Denegado</h1>
        <p>Lo sentimos, pero no tienes permiso para acceder a esta
página debido a un error en el servidor proxy.</p>
        <p>Por favor, contacta al administrador del servidor proxy
para obtener más información o <a href="#">inténtalo más
tarde</a>.</p>
    </div>
</body>
</html>
```

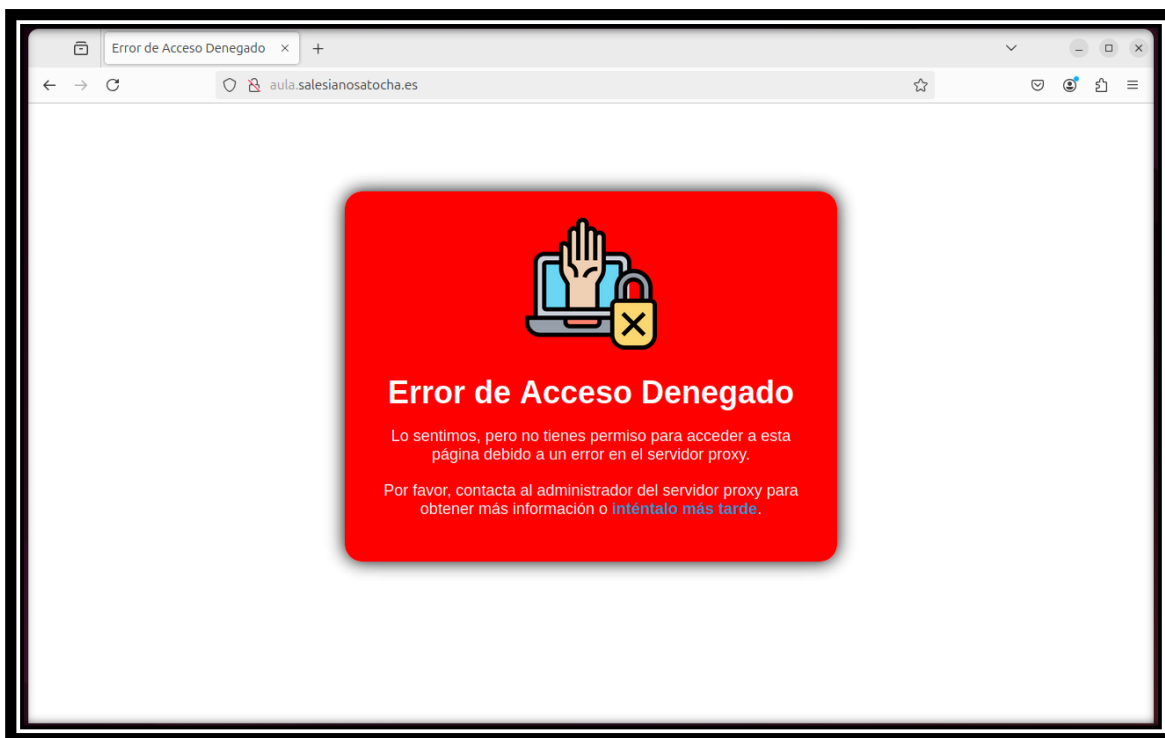
Lo pegamos en la siguiente ruta:

```
pc@pc-1:~$ sudo nano /usr/share/squid/errors/es-es/ERR_ACCESS_DENIED
pc@pc-1:~$
```



```
GNU nano 7.2 /usr/share/squid/errors/es-es/ERR_ACCESS_DENIED *
<body>
    <div class="error-container">
        
        <h1>Error de Acceso Denegado</h1>
        <p>Lo sentimos, pero no tienes permiso para acceder a esta página debid>
        <p>Por favor, contacta al administrador del servidor proxy para obtener>
    </div>
</body>
</html>
```

Obtendríamos una página de error tal y como esta:



INSTALACIÓN Y CONFIGURACIÓN DE SQUIDGUARD (AMPLIACIÓN)

Como ampliación, vamos a realizar la instalación y la configuración del servicio de SquidGuard (*SquidGuard, s.f.*). Es un servicio que también forma parte del squid proxy con el cual podemos restringir otras tantas páginas (ya sea de contenido de adultos, redes sociales, etc.).

Hacemos un **`sudo apt update`** y luego un **`sudo apt install squidguard`**.

```
pc@pc-1:~$ sudo apt install squidguard
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  squidguard-doc
```

Una vez hayamos instalado el servicio de SquidGuard, en el propio squid, vamos a habilitarlo.

Entraremos en la configuración de squid.

```
pc@pc-1:~$ sudo nano /etc/squid/squid.conf
```

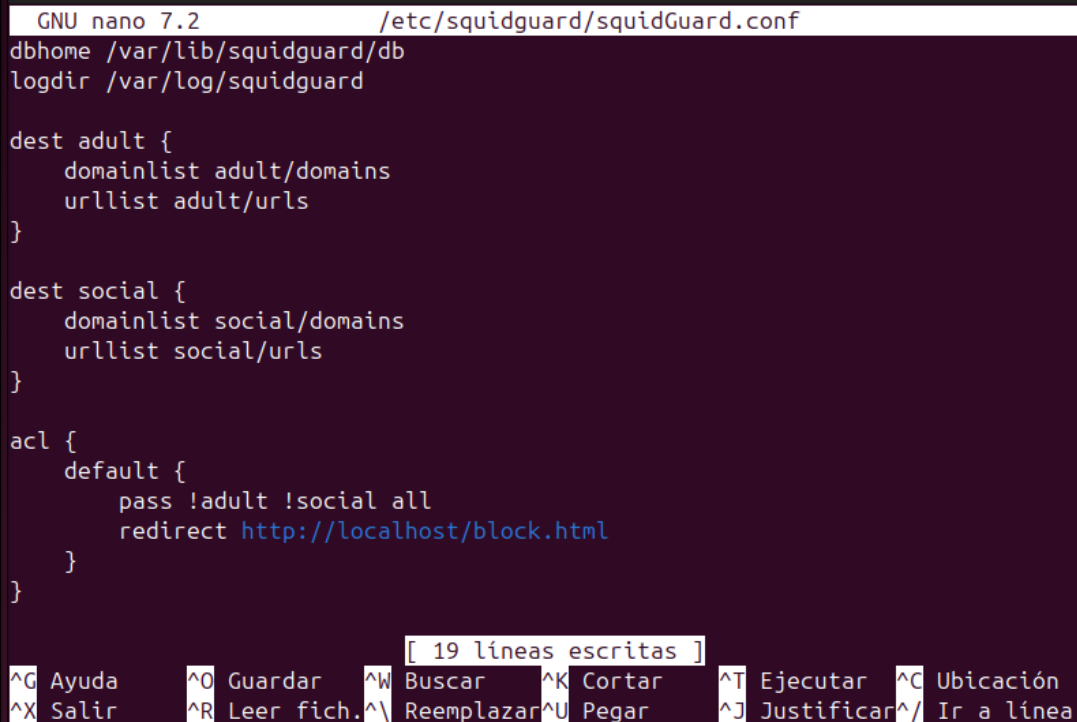
Dentro, antes de los acls, insertaremos las siguientes líneas:

```
# none

# Habilitar SquidGuard como redireccionador
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5

# TAG: acl
```

Una vez hayamos redireccionado SquidGuard a nuestro proxy, vamos a configurarlo. Entramos al archivo de configuración utilizando **sudo nano /etc/squidguard/squidGuard.conf**



```
GNU nano 7.2 /etc/squidguard/squidGuard.conf
dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

dest adult {
    domainlist adult/domains
    urllist adult/urls
}

dest social {
    domainlist social/domains
    urllist social/urls
}

acl {
    default {
        pass !adult !social all
        redirect http://localhost/block.html
    }
}
```

[19 líneas escritas]

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

Podemos observar un ejemplo de configuración básica para el SquidGuard. Una vez hayamos implantado esta configuración, vamos a proceder a descargar e instalar las listas negras (EIClickIzquierdo, s.f.).

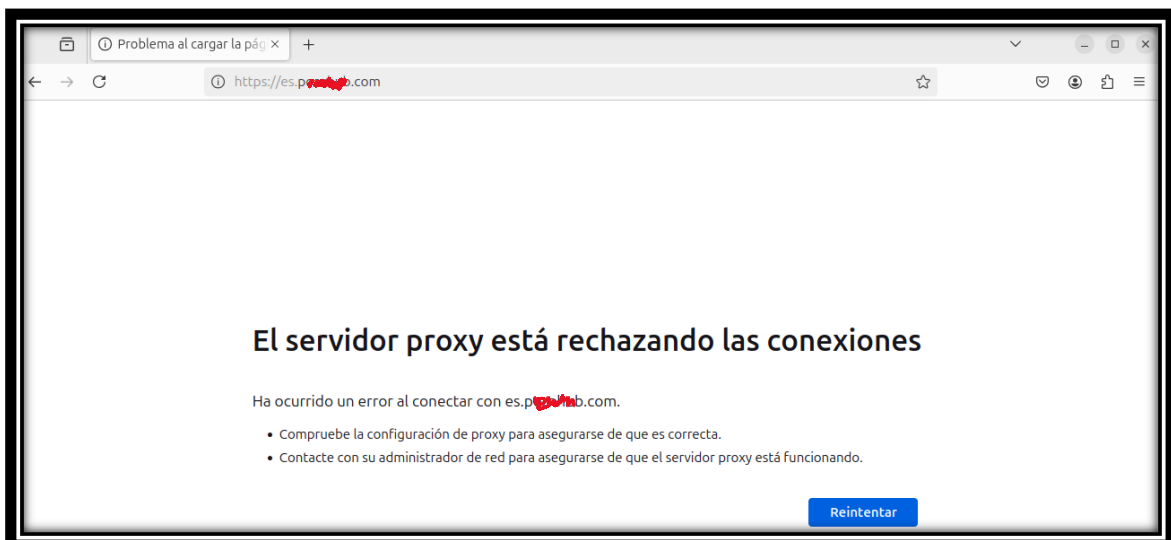
Utilizaremos las siguientes listas negras: http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

```
pc@pc-1:~$ sudo mkdir -p /var/lib/squidguard/db
pc@pc-1:~$ cd /var/lib/squidguard/db
pc@pc-1:/var/lib/squidguard/db$ sudo wget -o blacklist.tar.gz http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
```



```
pc@pc-1:/var/lib/squidguard/db$ sudo tar -xzf blacklists_for_pfsense.tar.gz.1
blacklists/
blacklists/README
blacklists/global_usage
blacklists/cc-by-sa-4-0.pdf
blacklists/LICENSE.pdf
blacklists/adult/
blacklists/adult/domains
blacklists/adult/expressions
blacklists/adult/urls
blacklists/adult/usage
blacklists/adult/very_restrictive_expression
blacklists/agresif/
blacklists/agresif/domains
```

Una vez realizado todo este proceso, reiniciamos squid y comprobamos que funcione la lista negra. En este ejemplo, utilizaremos una página destinada para adultos.



Podemos comprobar que, sin tener que ir bloqueando páginas manualmente, utilizando una lista negra mediante SquidGuard se puede bloquear infinidad de páginas no apropiadas (al igual que también podemos nosotros realizar una lista negra para bloquear páginas, tales destinadas para adultos, redes sociales, etc.).

CONCLUSIÓN

El proyecto ha logrado cumplir con los objetivos propuestos, implementando un servidor proxy con Squid y complementándolo con SquidGuard para proporcionar un control granular del acceso a Internet. La integración de estos componentes ha permitido optimizar el uso del ancho de banda, mejorar la seguridad y facilitar la administración del acceso a la web en la red interna. Gracias a la flexibilidad de Squid y la potencia de SquidGuard, la red ahora cuenta con un sistema de filtrado robusto, adaptable a futuras necesidades.

BIBLIOGRAFÍA

Clouding.io. (s.f.). Obtenido de Instalar Squid Proxy:

<https://help.clouding.io/hc/es/articles/5399482806556-Cómo-configurar-un-Servidor-Proxy-con-Squid-en-Ubuntu-22-04-LTS>

ElClickizquierdo. (s.f.). Obtenido de <https://elclickizquierdo.wordpress.com/wp-content/uploads/2008/07/informeproxy.pdf>

ProfeSantiago. (s.f.). *YouTube*. Obtenido de Bloquear páginas web Proxy:

<https://www.youtube.com/watch?v=pAxv7AtKupM>

SquidGuard. (s.f.). Obtenido de <https://www.ecured.cu/SquidGuard>

testdevelocidad. (s.f.). Obtenido de Ventajas y desventajas Proxy:

<https://www.testdevelocidad.es/2020/07/20/ventajas-desventajas-proxy/>

Ugustavo. (s.f.). *WordPress*. Obtenido de Modificar página web de error:

<https://ugustavo.wordpress.com/2011/04/06/cambiar-mensajes-de-error-en-squid/>

Wikipedia. (s.f.). Obtenido de Servidor Proxy: https://es.wikipedia.org/wiki/Servidor_proxy